Corr. WO 97/16904

[19]中华人民共和国国家知识产权局

[51]Int. Cl[6]
H04L 9/32

[12]发明专利申请公开说明书

[21]申请号 96199323.5

[43]公开日 1999年1月20日

[11]公开号 CN 1205818A

[22]申请日 96.10.31 [21]申请号 96199323.5
[30]优先权
[32]95.10.31 [33]SE [31]9503481-0
[86]国际申请 PCT/SE96/01396 96.10.31
[87]国际公布 WO97/16904 英 97.5.9
[85]进入国家阶段日期 98.6.25
[71]申请人 托达斯数据系统公司
地址 瑞典哥特伯格
[72]发明人 安德斯·约翰逊

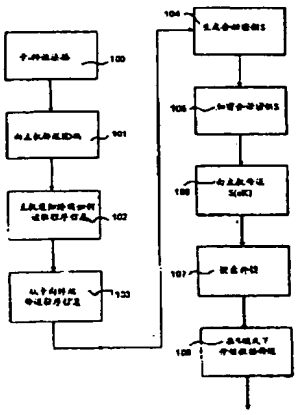
[74]专利代理机构 柳沈知识产权律师事务所
代理人 马 莹

权利要求书3页 说明书7页 附图页数13页

[54]发明名称 数据通信方法和设备

[57]摘要

一种用于在受IC卡(1)控制的终端、和诸如银行中央计算机的中央单元(3)之间安全传送数据的方法和系统。IC卡(1)包括:卡专用程序信息,该信息用于控制采用安全系统模式下的该卡与终端(2)之间的交互;卡专用保密信息,用于在安全系统模式下采用密码来保护终端(2)和中央单元(3)之间的数据传送。从该IC卡中不能读出存储的卡专用保密信息。出于所述控制的目的,将卡专用程序信息从该IC卡传送给该终端。



权 利 要 求 书

1. 一种在用户单元与中央单元之间传输数据的方法，所述用户单元包括一个终端以及一个被放置来与该终端通信的IC卡，所述中央单元例如一台安装在服务业者，特别是银行中的中央计算机，在所述用户单元和所述中央单元中使用保密信息来保护在所述单元之间传送的数据；所述方法的特征在于：

所述用户单元被设置在一个安全系统模式下工作，以便在所述用户单元和中央单元之间安全传送数据，以禁止未经授权的人得到传送数据的内容，和/或能够校验传送的数据是否在数据传送过程中被更改或替换；

利用将所述用户单元设置在安全系统模式下工作的所述卡中的卡专用程序信息来控制所述终端和所述卡的相互作用，所述卡专用程序信息被传送到要在所述控制下使用的所述终端；和

使用所述IC卡中的卡专用保密信息执行安全数据传送，使用卡专用保密信息来执行密码保护，防止从所述卡中遗失所述卡专用保密信息。

2. 如权利要求1所述的方法，其中，在通常系统模式下执行最初操作，以在所述终端和所述卡之间建立通信并且将所述卡专用程序信息传送给所述终端。

3. 如权利要求1至2中之一所述的方法，其中，根据从所述用户单元向所述中央单元传送的卡识别代码，所述中央单元指示所述用户单元要采用的从所述卡向所述终端传送所述卡专用程序信息的方式。

4. 如权利要求1至2中之一所述的方法，其中，根据所述终端和/或所述IC卡中包含的信息，在两者之间建立通信之前，传送所述卡专用程序信息。

5. 如权利要求1至4中之一所述的方法，其中，在所述用户单元中设立用于在安全系统模式下传送数据的会话密钥，在所述IC卡中对所述会话密钥加密或解密，其中以加密或解密的形式将所述会话密钥传送给所述中央单元。

6. 如权利要求1至4中之一所述的方法，在所述用户单元中设立一会话密钥，以明文将所述会话密钥传送给中央处理单元，然后在中央处理单元和所述IC卡中对所述会话密钥加密或解密，以便在安全系统模式下传送数据时以加密或解密的形式使用。

7. 如权利要求 5 或 6 所述的方法，其中所述会话密钥是最好在所述终端中产生的随机数。

8. 如权利要求 5 至 7 中之一所述的方法，其中一旦在所述卡和所述终端之间的连接中断，就删除所述用户单元中的所述会话密钥。

9. 如权利要求 5 至 7 中之一所述的方法，其中一旦在所述 IC 卡和所述终端之间建立新的连接，就删除所述用户单元中的所述会话密钥。

10. 如前面权利要求中之一所述的方法，其中仅在安全系统工作模式下通过与所述终端连接的键盘输入信息。

11. 一种数据传输的系统，包括：具有 IC 卡(1)和终端(2)的用户单元(1,2)、和中央单元(3)；所述卡(1)包括用于与所述终端(2)通信的通信装置(4)；所述终端(2)包括：用于与所述卡(1)通信的终端通信装置(5)，和用于与所述中央单元(3)通信的终端通信单元(6)；所述中央单元(3)包括用于与所述终端(2)通信的中央通信单元(7)；以及，所述用户单元(1,2)和所述中央处理单元(3)包括用于加密保护在所述各单元之间数据传送的保密信息；所述系统的特征在于：

所述 IC 卡(1)包括：第一卡存储装置(9)，用于存储卡专用程序信息；和，第二卡存储装置(10)，用于存储卡专用保密信息，该卡专用保密信息用于在安全系统模式下密码保护在所述用户单元和中央单元(3)之间的数据传送，所述第二卡存储装置(10)的结构使得不能从所述卡(1)读出所述保密信息；

所述终端(2)包括：终端读出装置(11)，用于读出所述第一卡存储装置(9)的内容；和程序执行装置(12)，用于使用读出的卡专用程序信息来控制所述终端(2)和所述 IC 卡(1)之间的相互作用，以便建立所述安全系统模式。

12. 如权利要求 11 所述的系统，其中，所述用户单元包括用于产生一会话密钥的密钥产生装置(13)，存储该会话密钥的存储装置(14)，并且所述 IC 卡(1)包括用于密码保护所述会话密钥的处理装置(15)，所述会话密钥由所述终端通信单元(6)传送给所述中央单元。

13. 如权利要求 12 所述的系统，其中所述密钥产生装置(13)是随机数产生器或伪随机数产生器。

14. 如权利要求 12 或 13 所述的系统，其中所述密钥产生装置(13)设置在所述终端(2)中。

15. 如权利要求 12 或 13 所述的系统，其中所述密钥产生装置构成所述处理装置(15)的组成部分。

16. 如权利要求 12 至 15 中之一所述的系统，其中，一旦在所述卡通信装置(4)和所述终端通信装置(5)之间的连接中断，所述用户单元就删除中所述用户单元中的所述会话密钥。

17. 如权利要求 12 至 15 中之一所述的系统，其中，一旦在所述卡通信装置(4)和所述终端通信装置(5)之间建立新的连接，所述用户单元就删除中所述用户单元中的所述会话密钥。

18. 如权利要求 11 至 17 中之一所述的系统，其中，所述 IC 卡(1)包括用于存储要传送给所述中央单元(3)的卡识别信息或卡识别代码的存储装置(16)；所述中央单元在所述代码或信息的引导下指示所述用户单元(1,2)读出所述第一卡存储装置(9)内容的方式。

19. 如权利要求 11 至 18 中之一所述的系统，其中，所述用户单元包括用于向所述系统输入数据的键盘，所述键盘仅在所述系统处于安全系统模式下时工作。

说　明　书

数据通信方法和设备

本发明涉及在一中央单元或主机和用户单元之间进行数据通信的方法和设备，例如，该中央单元或主机可以是银行中的中央计算机，该用户单元包括：用户携带的 IC 卡，当他想要与主机进行与通信有关的事项处理时使用该 IC 卡；能够与 IC 卡和主机通信的终端，它作为在 IC 卡和主机之间的互联链路。

目前均知道使用的数据传输系统包括 IC 卡控制终端和一个主机；同样也知道，在一些系统中使用某种保密信息，采用密码保护传输的数据。

在现今使用的数据传输系统会发现两个最主要的缺点，首先一个是终端所包含的秘密信息由于这些终端对于公众实际上可获得，事实上会被暴露而侵害到其内部秘密，因为一些未被授权的人会从终端上努力去读懂这些秘密信息；第二个缺点是因为目前 IC 卡配置标准，除了一些基本特性如信号电平等等，对诸如数据将被分配到那些存储地址上允许有相当的自由度，所以终端通常只能处理一种形式的卡。

本发明的目的是提供一种解决或从相当程度上消除上述列举问题的方法和系统，从而提高在系统中的卡使用方面的通用性，并增加在管理秘密信息上的安全性。

本发明的目的通过权利要求 1 限定的方法和权利要求 11 限定的系统来实现。

本发明基本概念是至少在用户单元和主机之间传输敏感数据通过单独的安全系统模式来实现，安全系统模式的程序控制实现是采用包含在卡中的卡专用程序信息来完成；安全系统模式意味着所执行的数据传输的方式，使非经授权的人不能在其干扰行为不被发现的情况下歪曲或操纵被传输的数据；基于这种目的，秘密信息在用户单元和主机间被使用，而在卡与终端间通讯的初始化操作在所谓正常系统模式下执行。

根据本发明所采用的卡带有的卡专用程序信息，传送给终端，而终端使用它来建立安全模式。

根据本发明在终端中的“驻留”程序内容只是绝对必需的信息，每张卡

带有的程序信息是给某个人卡专用的，并会传送给终端；由于卡专用程序信息被传送给终端，后者不必含有专门对每张个人卡或某种卡的“驻留”程序信息。

这就使得在系统中可使用不同方式配置的卡，而且终端不必包含相当多的软件；并且例如，几种卡的发行者可以使用同一类终端，而终端不必包含，或其它卡发行者不必知道，某特定卡发行者采用的安全系统模式所使用的软件。

依据本发明的系统制造的终端既不昂贵，同时具有“灵活性”，即可以毫无困难地使不同配置的卡与终端相适应，且终端也不用改变或被提供有新的“驻留”程序信息。

按照本发明的一实施例，在主机的控制之下，执行从卡上向终端传送卡专用程序信息，主机的控制是基于由用户单元传送的卡鉴别信息或代码。然而，显然这种终端和卡之间的信息传送也可以不涉及主机。

依据本发明使用的卡还含有卡专用保密信息，用于产生数据传输的保护密码，并且不可能从卡上读出存储的该保护密码。

按照优选实施例，卡专用保密信息用于通过最好是所谓的 DES 算法来加密（从广义来讲）最好是以随机数形式生成的会话密钥，然后以加密的形式将会话密钥传送给主机。然后，在安全系统模式下，利用此会话密钥来密码保护用户单元和主机之间的数据传送。

最迟要在下一次某 IC 卡和该终端之间建立联系时，在用户单元中删除以上提及的会话密钥，虽然在因想要开始新的会话而仍保持联系或当所涉及的卡和该终端之间的联系中断时都可以执行此种删除。

很明显，同样在安全系统模式下可以采用卡专用保密信息等，来密码保护在主机和用户单元之间的数据传送，即该保密信息可以用作加密算法或识别算法中的密码密钥。

按照一优选实施例，终端包含一个仅在安全系统模式下使用的键盘。

为了保护在开放线路上或在未经授权人也可访问的其它媒介中传送的数据，使用了多种不同的加密技术。一种常用的方法是首先加密数据然后再传送最后解密；与其颠倒的顺序也可以，即首先解密，然后传送，最后加密传送的数据，然后以明文恢复数据。显然所采用的这两种技术与本发明相关。举例来说，若采用一个随机数来在加密算法中生成加密密钥，则可以不以明

文传送随机数，而对其加密/解密后，将所得结果作为加密密钥来使用．所采用的此技术也与本发明有关，所以它不能限制本文中详细描述的加密技术的应用．对称和非对称加密系统均可被使用．

图 1 是本发明系统一实施例的示意框图；

图 2 示出一优选实施例的在安全模式下用户单元和主机之间的数据传送初始化之前采取措施的流程图；

图 3 示出本发明的在向主机传送密钥之前密钥生成和加密的方式；

图 4 示出本发明优选实施例的报文（数据）的识别；

图 5 示出生成代码密钥且将其传送给主机的多种不同情况的表格；

图 6A 至 6H 为图 5 中所列各种方式的流程图．

参考图 1，以下将描述设计用于安全传送数据的系统，它包括用户单元和中央单元 3（主机），用户单元包括 IC 卡 1、终端 2．

IC 卡 1 包括卡通讯装置 4，它与终端通讯装置 5 相连接，使 IC 卡 1 和终端 2 建立起用于数据传输的连接．

另外，IC 卡 1 包括：第一卡存储装置 9，用来存储要传送给终端 2 的卡专用程序信息；第二卡存储装置 10，用来存储卡专用保密信息，使得不能从卡上读出该信息；存储装置 16，用来存储卡识别代码；以及，处理器 15．如下所述，处理器 15 包含允许执行所需密码处理（在此情况下是加密）和在会话密钥传送给主机 3 之前生成会话密钥所需的程序信息．

终端 2 包括：终端通讯单元 6，用来同与主机 3 相连的中央通讯单元 7 通讯，以实现主机 3 与用户单元之间的数据传送；密钥生成装置 13，用于以随机数或伪随机数生成器的形式生成一个会话密钥，然后该会话密钥以加密状态传送给主机，用来识别在用户单元和主机 3 之间传送的报文，如下所述．终端 2 还包括存储会话密钥的存储装置 14．

按照另一优选实施例，在终端中没有采用密钥生成装置，而是在卡中处理器 15 中生成密钥．

除了在按照本优选实施例被认为已采用的安全系统模式下将会话密钥传送给主机的系统传送之外，终端 2 和主机 3 还包括控制其它模式下系统传送的控制装置 8 和 18．在这种模式下，在终端 2 和主机 3 之间的数据传送方式，是使通过已传送给主机的会话密钥来保护（通过密码识别）正被传送的数据．另外，终端 2 包括读出装置 11，用来读出所述第一卡存储装置 9 中的

卡专用程序信息，读出的程序信息被存入且被终端 2 中的程序执行装置 12 所使用，以便控制终端 2 和 IC 卡 1 之间的交互.

图 2 以流程图的形式示出按照一实施例在安全系统模式下传送数据开始之前 IC 卡、终端和主机相互协作的方式. 参照图 4 在以下将更详细地说明处理过程.

在步骤 100， IC 卡 1 插入终端 2，从而在所述终端通讯装置 5 和所述卡通讯装置 4 建立联系；在步骤 101，一个存在所述存储装置 16 中的 ID 码从用户单元的 IC 卡经终端 2 传送给主机 3；在步骤 102，根据识别出的卡类型即卡的配置，主机 3 通知终端 2，怎样使用其读出装置 11 来从所述第一卡存储装置 9 中读出卡专用程序信息. 按照已优选实施例，由主机传送的数据包含读出操作起始地址信息. 在步骤 103，卡专用程序信息从卡 1 中读出给终端 2. 在步骤 104，在所述密钥生成装置 13 中生成一个随机数，当采用报文识别算法（ MAA ）时，所述随机数在密封处理中用作会话密钥. 在步骤 105，利用 IC 卡 1 的所述第二卡存储装置 10 中包含的保密信息，在所述加密装置 15 中加密在 IC 卡中的会话密钥；在步骤 106，会话密钥以加密状态传送给主机 3. 在图 3 中更详细说明了步骤 104、 105 和 106. 在步骤 107，与终端 2 联结的一个键盘解锁供使用. 在步骤 108，数据传送在目前采用的安全系统模式下开始进行.

以下参照图 3 进行叙述. 按照该优选实施例，在终端生成的一个随机数用作 MAA 处理的密钥，来识别从用户单元传送给主机的报文或从主机传送给用户单元的报文. 然后，利用所述第二卡存储装置 10（ 图 1 ）中的保密信息（ DES 密钥）作为加密钥匙，用 DES 加密算法在卡中加密此随机数，以便将加密后的随机数（它由 eK 表示）在加密状态下经终端传给主机 3，在主机 3 上该随机数被解密，并作为 MAA 中的会话密钥.

图 4 举例说明按照该优选实施例在安全系统模式下执行数据传送和数据识别的方式. 加密的随机数 ek 已从用户单元传送到主机，在主机中利用主机中存储的密钥被解密，所述密钥取决于正被使用的卡并与所述卡中的密钥相同. 然后，在 MAA 中，解密后的随机数用作一个 MAA 密钥，并与要传送给用户单元的报文、报文序列号一起生成密码检查和，即报文识别码（ MAC ），加在报文中用来识别报文. MAC 在同一会话的连续报文中有不同的形式（尽管它们内容是一致的，但它们被加入不同的序列号）. 所以，被

传送的数据流包括：报文、序列号、明文、 MAC .

在用户单元，终端使用 MAA 密钥即所述随机数进行一个 MAA 检查，核实收到的报文，或换句话说，检查已核实从主机到用户单元传送中该报文是否被更动．该检查包括确定一致性的 MAC 相应计算、与报文一起收到的 MAC 的 MAC 比较。

当用户单元准备向主机传送一响应报文时，主机以相应方式进行一处理，即该主机在所述随机数、该响应报文、和从该主机传送的序列号的基础上计算一新的 MAC，该新的 MAC 被加入到来自用户单元的响应和传送自主机的最后序列号所形成的数据流中．然后，主机对传送响应进行一 MAA 检查，以检查在用户单元至主机的传送过程中该响应数据是否被更动．以后的报文传送也以同样方式进行．

图 5 是一些本发明可以使用的随机数产生和随机数保护的可能情况 1-8 的表。所示的四种情况（ 1， 3， 5， 6 ）中，在终端中生成用作会话密钥的随机数；而所示的另四种情况（ 2， 4， 7， 8 ）中，在卡中生成随机数．另外，在表中所示的四种不同变化中，分别用于密码保护的相应会话密钥被传送给主机。

图 6A-6H 更详细地显示了图 5 中的 8 种不同情况．用于说明每种情况的各个步骤由白矩形框中的数字标号来指示．每幅图说明当用户将他的卡插入终端并且系统将工作于安全模式时所发生的情况．图中表明在所有 8 种情况中步骤 S1-S5 都是相同的．在步骤 S1 中，中央单元（主机）命令终端（终端）来读出卡的识别号以鉴别是否卡与所涉及的主机相关，并且当鉴别回答肯定时，提供与该卡相关的加密密钥，将其传送给主机，在主机中将使用它对随机数（会话密钥）进行加密或解密（这取决于该加密密钥以什么形式被传送给主机）．在步骤 S2，终端将读出的卡的号码传送给主机．在所有 8 种情况中，主机应确保该卡是由此主机的用户发行的，因此在步骤 S3 中它命令终端开始采用一种安全模式．在步骤 S4 和步骤 S5 中，终端执行它的驻留程序信息的程序系列，即从卡中的文件（ SMIB ）里读取卡专用程序信息．为了要采用安全模式而执行的其余步骤由 SMIB 即卡专用程序信息的内容控制．这表明，一个相对简单便宜的终端（原则上只能用于从 IC 卡中读取文件），当用在本发明的系统中时，在与不同方式配置的卡相互作用方面可以获得相对于其能力的令人惊讶的灵活性．第一种情况在图 3 中已有说明，即，在终

端中生成要用作会话密钥的随机数，在步骤 S6 中，在被传送到终端之前在卡中对该随机数加密，并且在步骤 S7 在终端中存储传来的该随机数，在步骤 S8 中，该终端最终将加密的随机数传送给主机，在这以后依据图 4 开始在安全系统模式下进行数据传送。

除了已经描述的步骤 S1-S5 之外，在所示的第二情况下，还要执行下述步骤，即：在步骤 S62 中，终端（根据相应 SMIB 的内容）命令卡生成一个随机数；在步骤 S72 中，卡生成并发送一随机数给终端并在其中存储；在步骤 S82 中，终端命令卡给生成的随机数加密；卡加密该随机数并以加密状态将其传送给终端；最后在步骤 S102 中，终端发送该加密随机数给主机，在这以后依据图 4 在安全系统模式下开始进行数据传送。

在所示的第三种情况中，除了上述已经描述的步骤 S1-S5 以外，还执行下面的步骤，即：在步骤 S63 中，终端生成并存储一个随机数，命令卡对随机数解密；在步骤 S73 中，将解密后的随机数发送给终端；在步骤 S83 中，发送解密随机数给主机。当随机数（会话密钥）到达主机时，在使用前不应解密而应加密该随机数，以便给明文提供密钥，然后依据图 4 方式在安全系统模式下开始进行数据传送。

在所示的第四种情况中，除了上述已经描述的步骤 S1-S5 之外，还执行下面的步骤，即：在步骤 S64 中，命令卡生成一个随机数；在步骤 S74 中，该随机数传送给终端并在其中存储；在步骤 S84 中，终端命令卡给该随机数解密；在步骤 S94 中，卡传送解密随机数给终端；最后在步骤 S104 中，解密随机数被发送到主机。当该随机数（会话密钥）到达主机时，在使用前不应解密而应加密该随机数，以便给明文提供密钥，然后依据图 4 方式在安全系统模式下开始进行数据传送。

在所示的第五种情况中，除了在已经描述的步骤 S1-S5 以外，还执行下面的步骤，即：终端生成一随机数，在步骤 S85 中以明文发送给主机，并且在步骤 S65 中被卡加密；在步骤 S75 中，发送加密随机数给终端并在其中存储。因为终端里有一个加密的会话密钥，并且该会话密钥以明文的形式传送给主机，为了要在安全系统模式下进行数据传送，需要在能使用会话密钥之前在主机中加密会话密钥。

所示的第六种情况与第五种情况的区别仅在于，每当在第五种情况中执行加密时，在第六种情况中要进行解密。

在所示的第七种情况中，除了已经描述的步骤 S1-S5 以外，还执行下面的步骤，即：在步骤 S67 中，终端命令卡生成一个随机数；在步骤 S77 中，发送该随机数给终端；在步骤 S107 中，该随机数以明文传送给终端，并且在步骤 87 中，卡给该随机数加密；最后在步骤 S97 中，加密的随机数被发送到终端并在其中存储．因为在终端中有加密的会话密钥，并且该会话密钥已经以明文被传送给主机，为了在安全系统模式下进行数据传送，在可使用会话密钥之前需要在主机中对会话密钥加密．

第八种情况与第七种情况的区别仅在于，每当在第七种情况中进行加密时，在第八种情况中进行解密．

根据图 5（图 6A）中的第一种情况，一组卡专用程序信息从卡传送给终端，使会话密钥产生，并由此传送给主机，这一过程的例子可包括下面一系列的命令：OPEN（打开卡中包含卡专用程序信息的文件，容许它在加密算法中被当作加密密钥使用），RANDOM（在终端的密钥生成装置 13 中，根据包含于命令中的指令产生一随机数，并将其存储在终端存储装置 14 中），CRYPT（将随机数读到卡上，处理器 15 中利用其中规定的一种常规加密算法对卡中的该随机数加密），READ（读出加密后的随机数给终端），以及 TRANS(将加密后的随机数传送给主机)．

应当指出，所定义的命令和函数只是示范性的，它们还可以采用很多不同的方式和以很多不同的编程语言来实现．在理解本发明时，对本领域普通技术人员来说，以程序代码形式在本发明的实施例中采用的函数实现的方法应是不言自明的，因此，在此没有对它们进行更详细的描述．

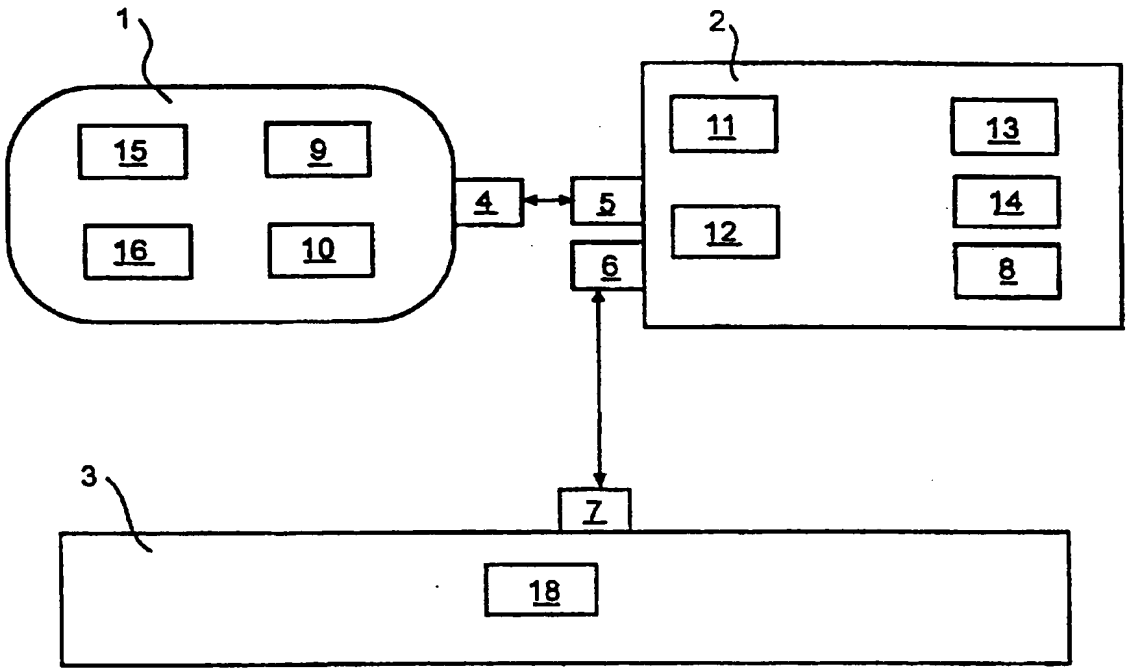


图 1

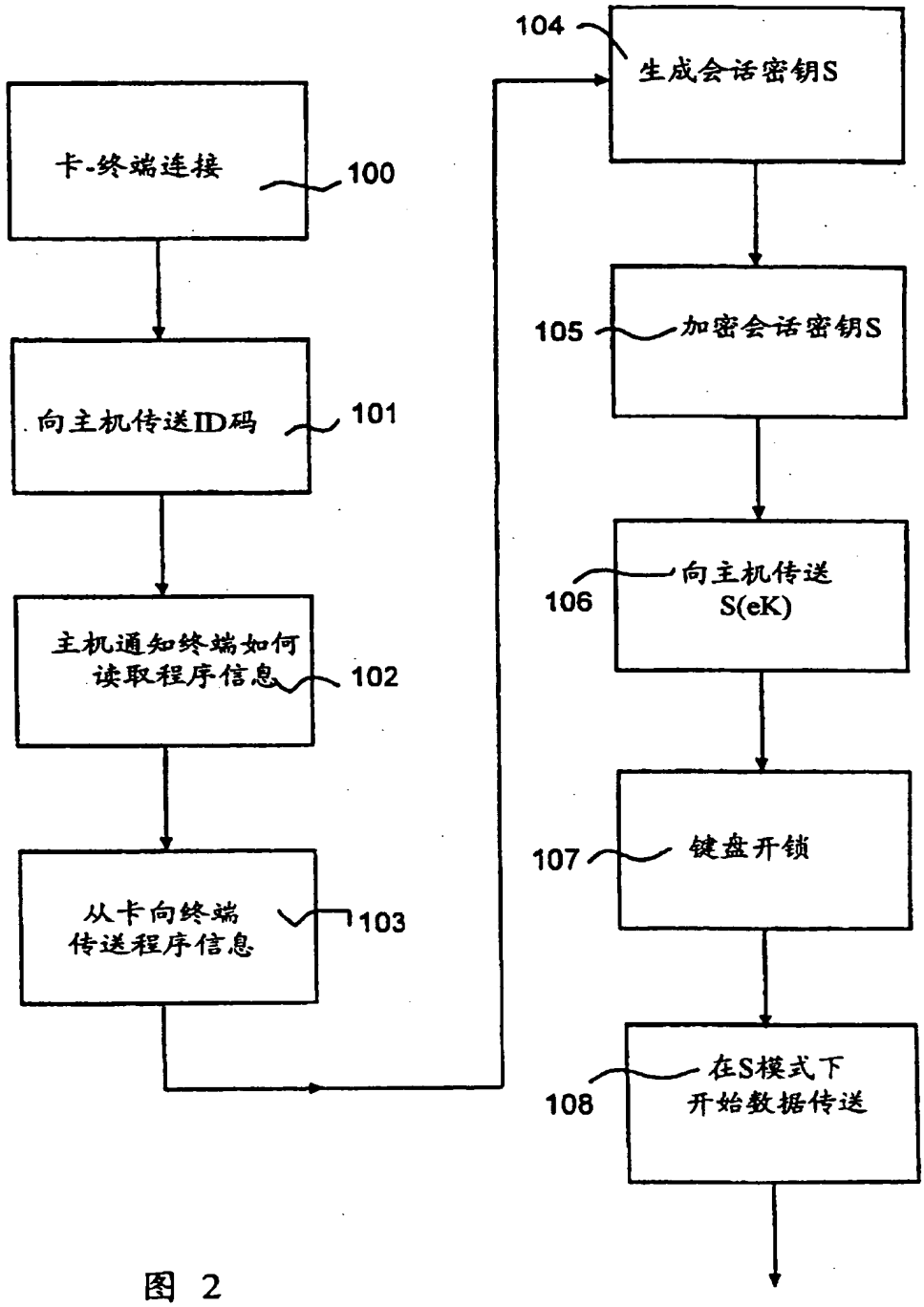

卡-终端连接
100
向主机传送ID码
101
主机通知终端如何
读取程序信息
102
从卡向终端
传送程序信息
103
104
生成会话密钥S
105
加密会话密钥S
106
向主机传送
S(eK)
107
键盘开锁
108
在S模式下
开始数据传送

图 2

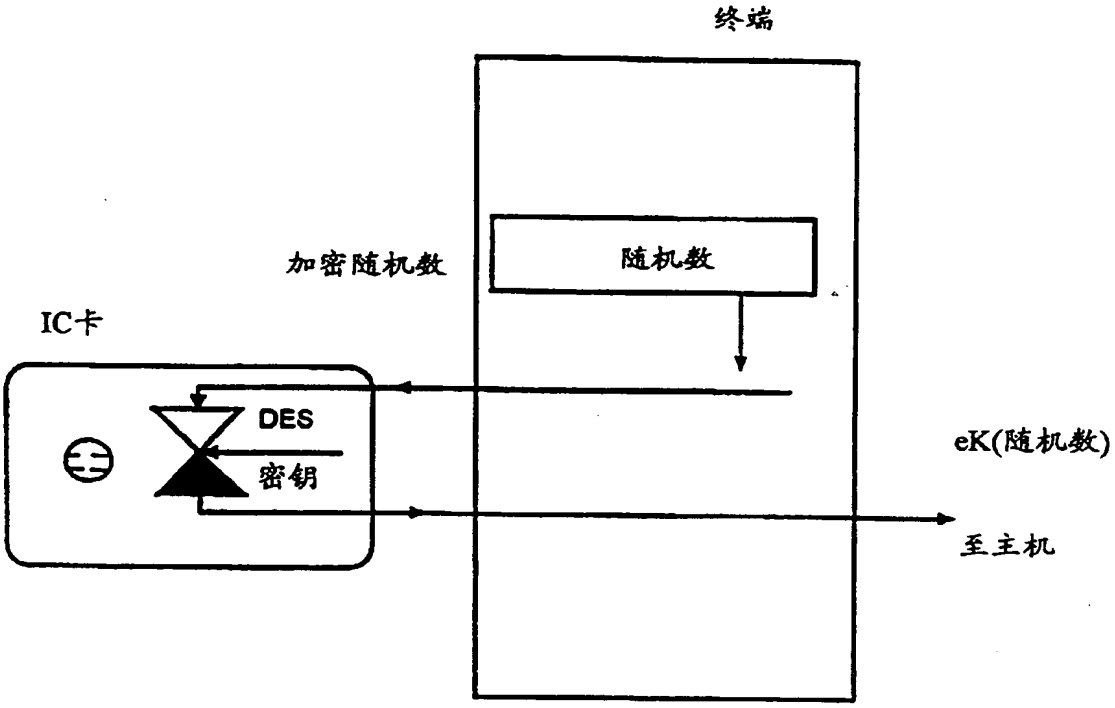


图 3

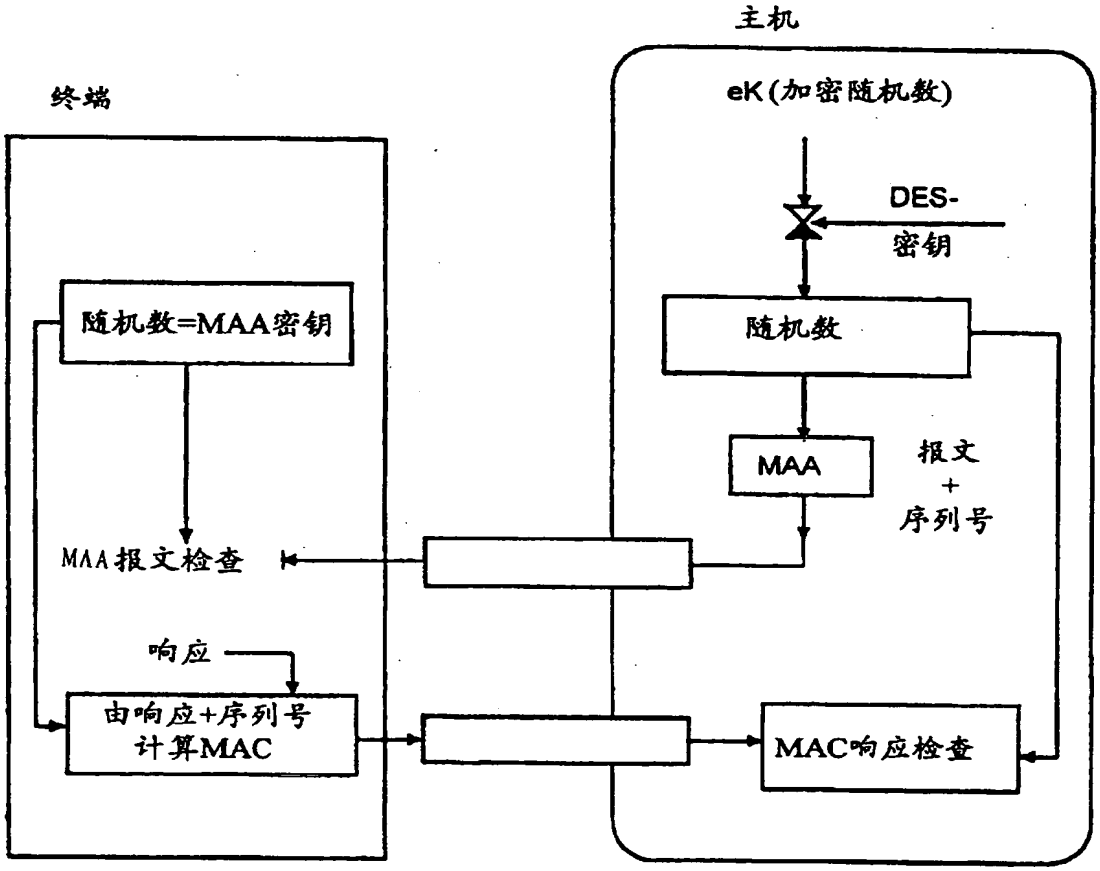

主机
终端
eK(加密随机数)
DES-
密钥
随机数=MAA密钥
随机数
MAA
报文
+
序列号
MAA报文检查
响应
由响应+序列号
计算MAC
MAC响应检查

图 4

情况	在何处产生随机数	在终端存储和使用随机数的方式	向主机传送随机数的方式	在主机使用前接收值的方式
1	终端	明文	加密	解密
2	卡	明文	加密	解密
3	终端	明文	解密	加密
4	卡	明文	解密	加密
5	终端	加密	明文	加密
6	终端	解密	明文	解密
7	卡	加密	明文	加密
8	卡	解密	明文	解密

图 5

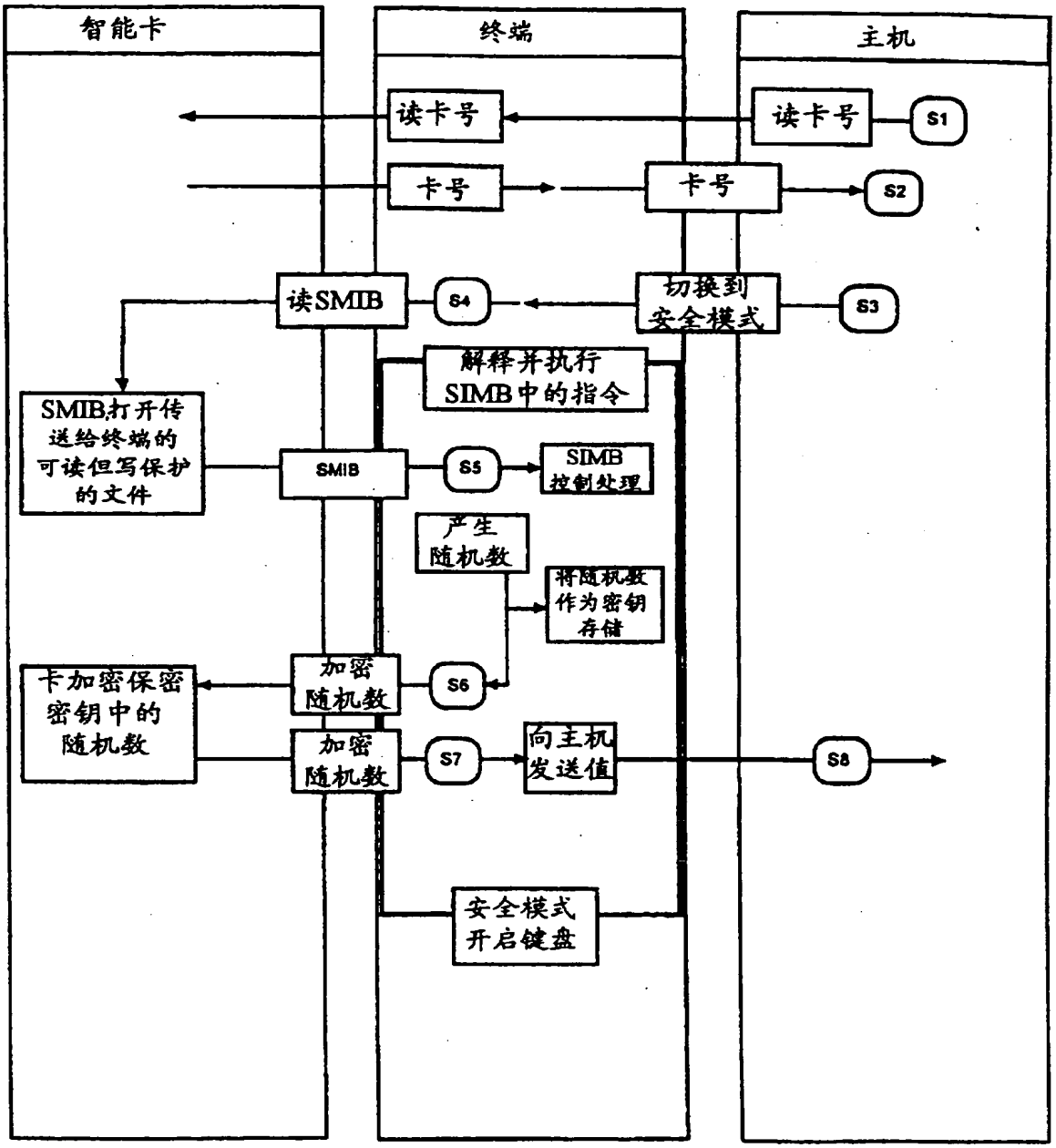

智能卡
终端
主机
读卡号
读卡号
S1
卡号
卡号
S2
读SMIB
S4
切换到
安全模式
S3
解释并执行
SIMB中的指令
SMIB打开传
送给终端的
可读但写保护
的文件
SMIB
S5
SIMB
控制处理
产生
随机数
将随机数
作为密钥
存储
卡加密保密
密钥中的
随机数
加密
随机数
S6
加密
随机数
S7
向主机
发送值
S8
安全模式
开启键盘

图 6A

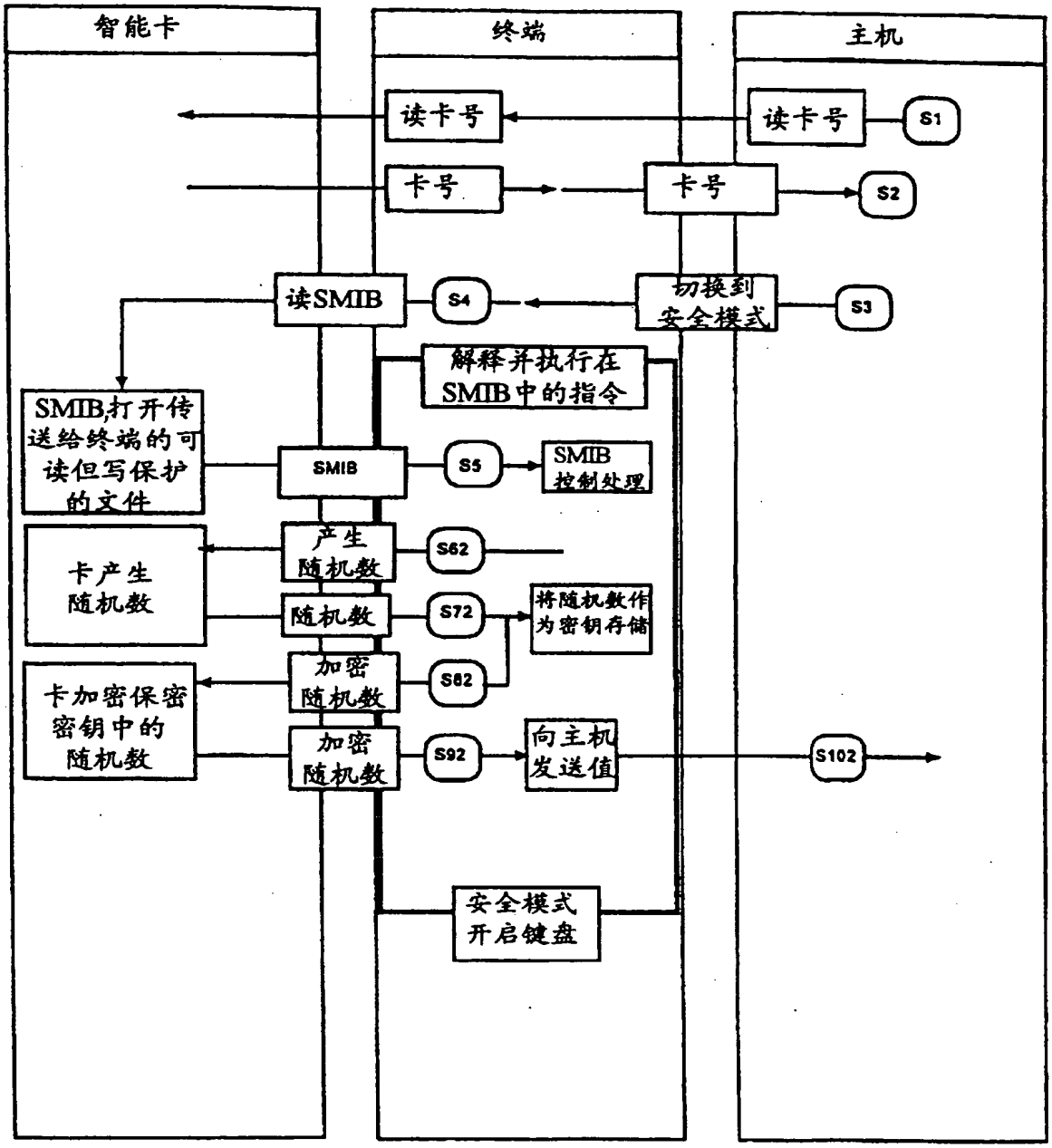

智能卡
终端
主机
读卡号
读卡号
S1
卡号
卡号
S2
读SMIB
S4
切换到
安全模式
S3
解释并执行在
SMIB中的指令
SMIB,打开传
送给终端的可
读但写保护
的文件
SMIB
S5
SMIB
控制处理
卡产生
随机数
产生
随机数
S62
随机数
S72
将随机数作
为密钥存储
卡加密保密
密钥中的
随机数
加密
随机数
S82
加密
随机数
S92
向主机
发送值
S102
安全模式
开启键盘

图 6B

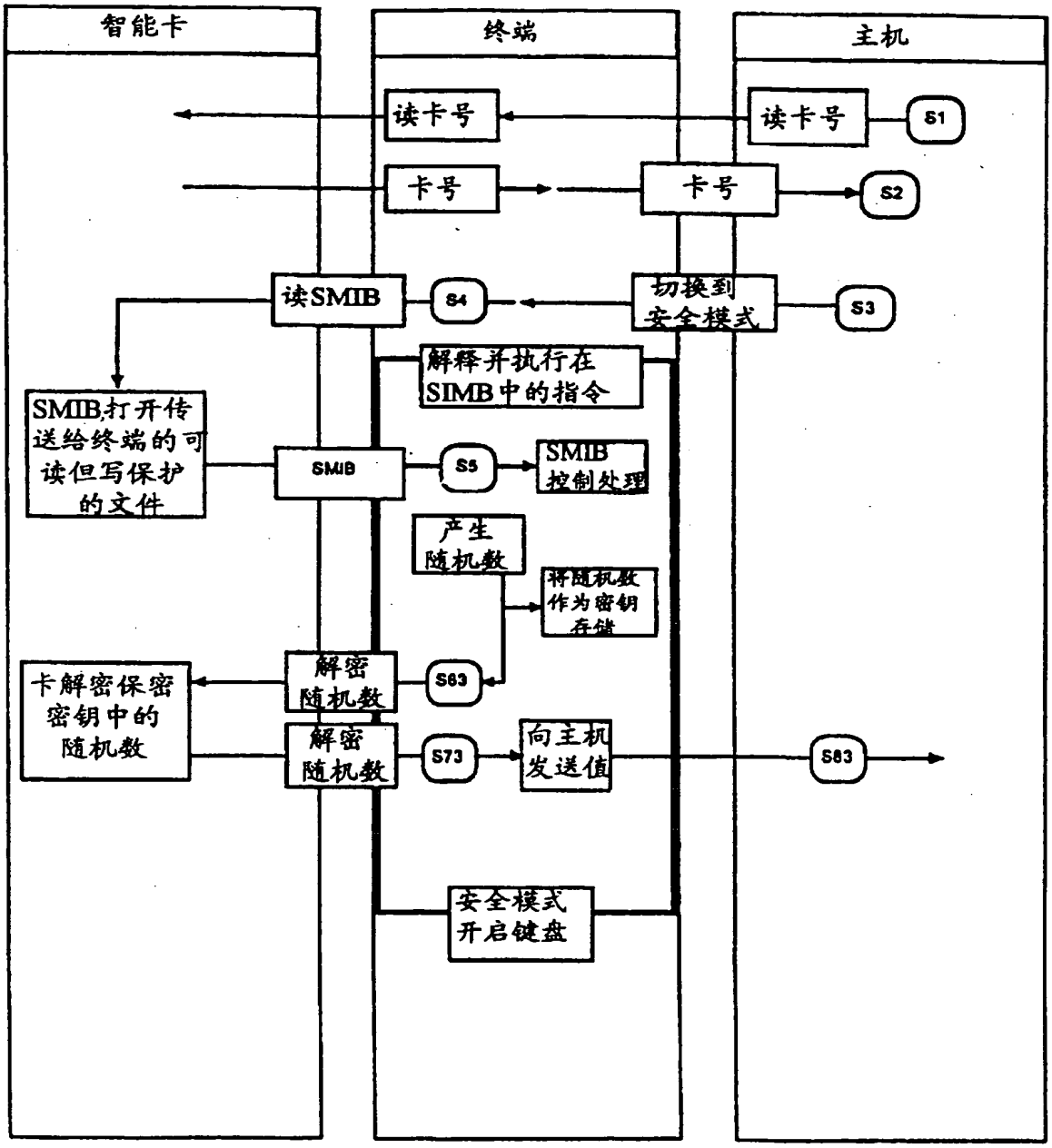

智能卡
终端
主机
读卡号
读卡号
S1
卡号
卡号
S2
读SMIB
S4
切换到
安全模式
S3
解释并执行在
SIMB中的指令
SMIB打开传
送给终端的可
读但写保护
的文件
SMIB
S5
SMIB
控制处理
产生
随机数
将随机数
作为密钥
存储
卡解密保密
密钥中的
随机数
解密
随机数
S63
解密
随机数
S73
向主机
发送值
S83
安全模式
开启键盘

图 6C

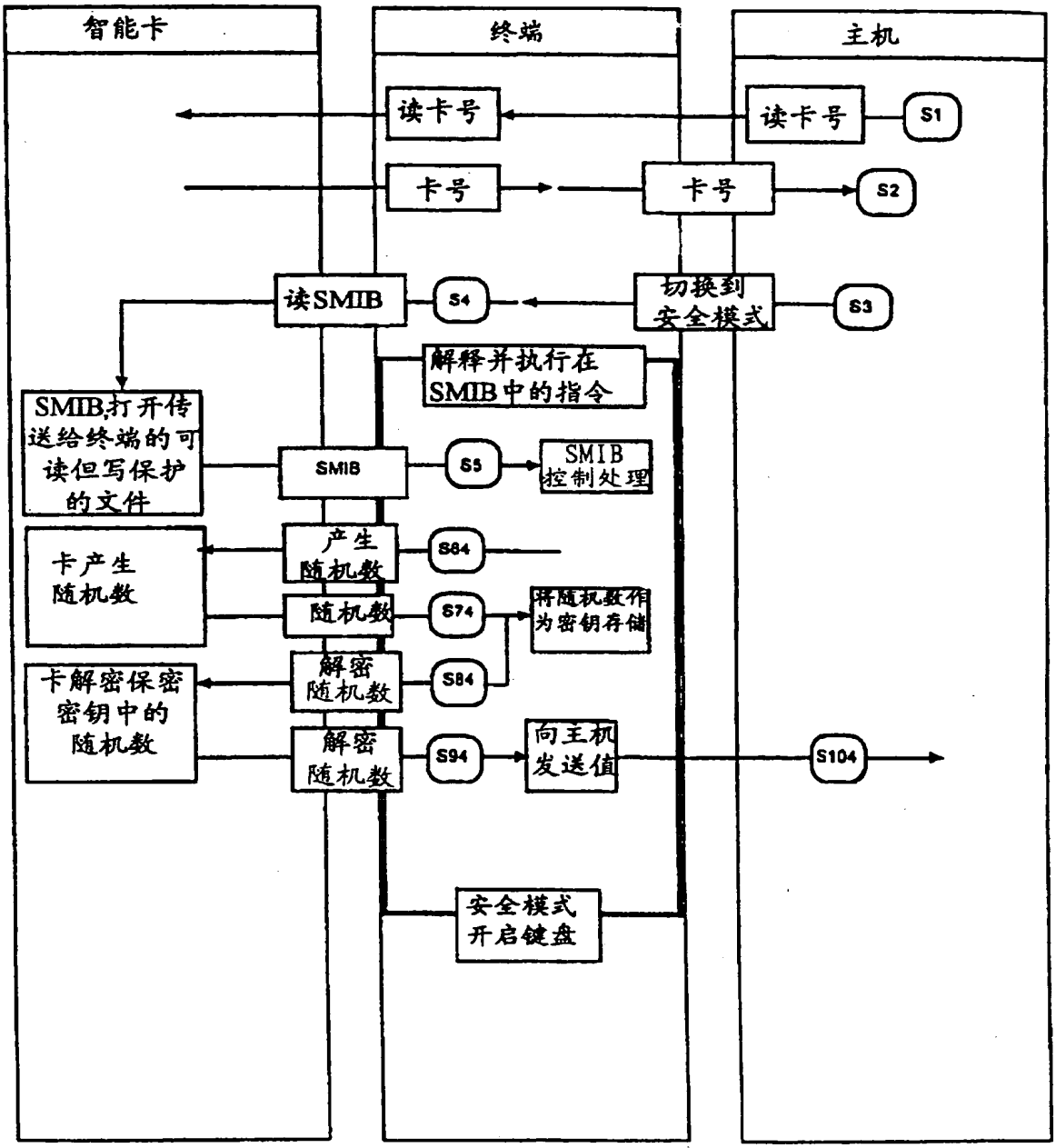

智能卡
终端
主机
读卡号
读卡号
S1
卡号
卡号
S2
读SMIB
S4
切换到
安全模式
S3
解释并执行在
SMIB中的指令
SMIB打开传
送给终端的可
读但写保护
的文件
SMIB
S5
SMIB
控制处理
卡产生
随机数
产生
随机数
S84
随机数
S74
将随机数作
为密钥存储
卡解密保密
密钥中的
随机数
解密
随机数
S84
解密
随机数
S94
向主机
发送值
S104
安全模式
开启键盘

图 6D

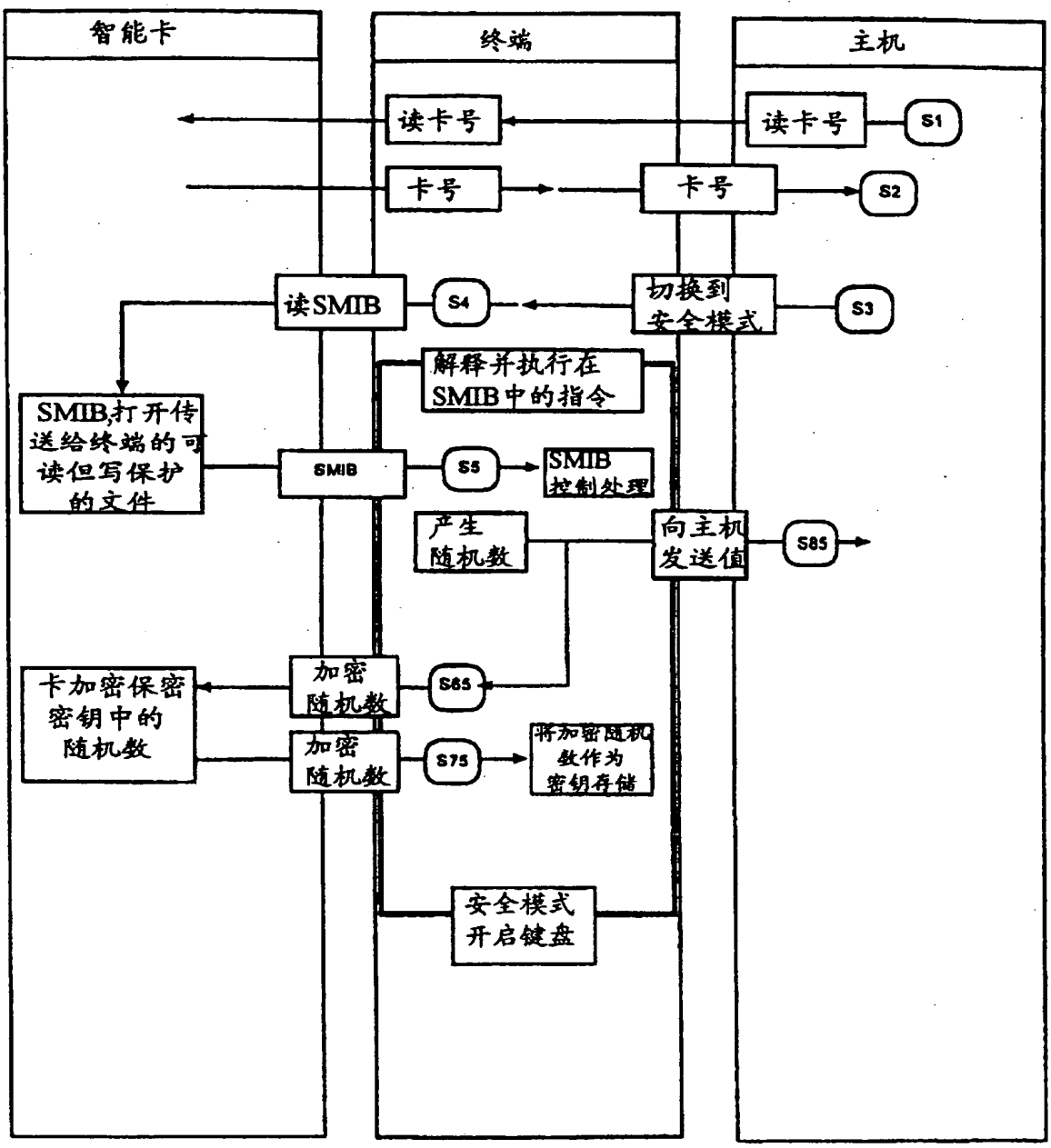

智能卡
终端
主机
读卡号
读卡号
S1
卡号
卡号
S2
读SMIB
S4
切换到
安全模式
S3
解释并执行在
SMIB中的指令
SMIB,打开传
送给终端的可
读但写保护
的文件
SMIB
S5
SMIB
控制处理
产生
随机数
向主机
发送值
S85
卡加密保密
密钥中的
随机数
加密
随机数
S65
加密
随机数
S75
将加密随机
数作为
密钥存储
安全模式
开启键盘

图 6E

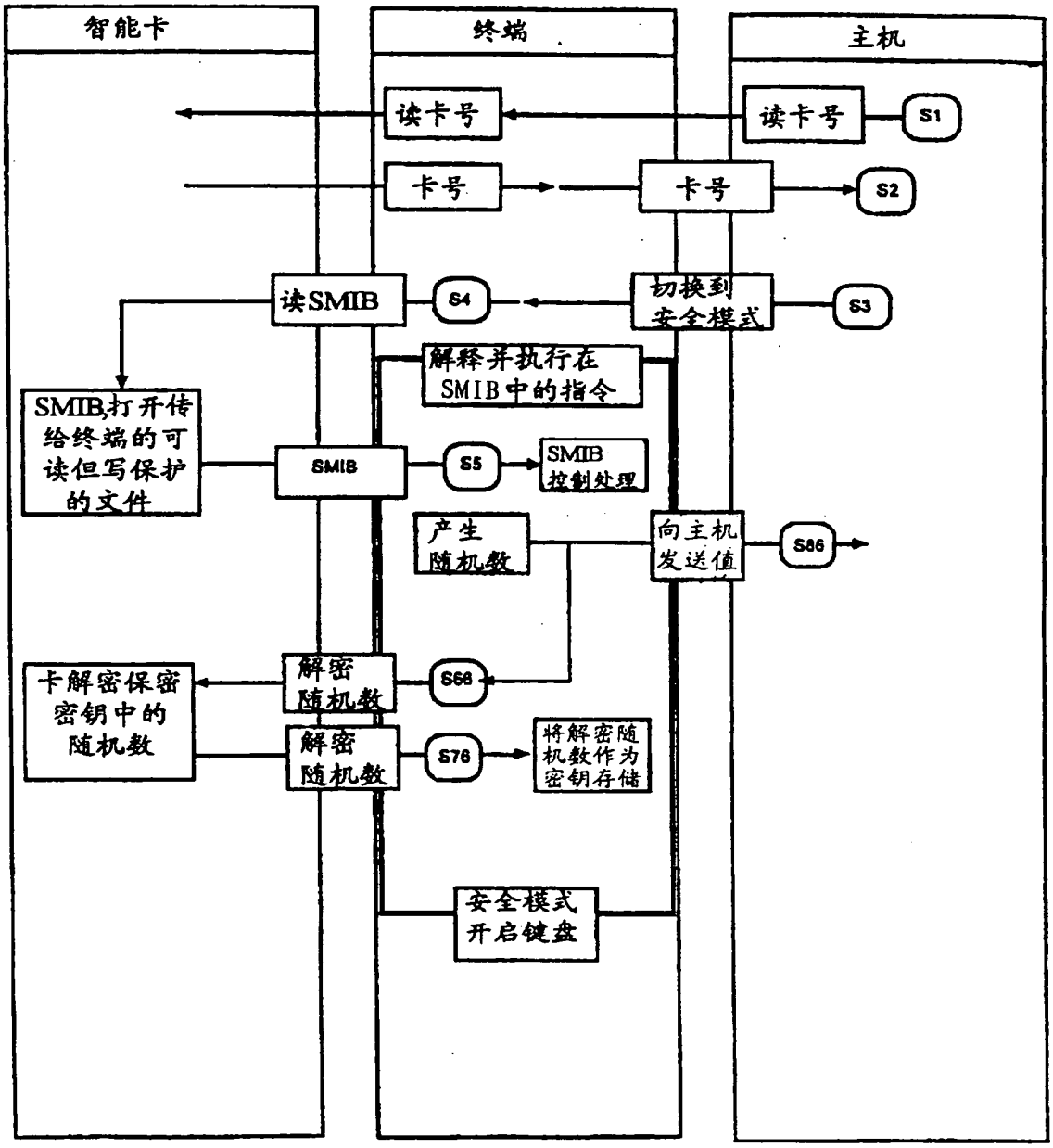

智能卡
终端
主机
读卡号
读卡号
S1
卡号
卡号
S2
读SMIB
S4
切换到
安全模式
S3
解释并执行在
SMIB中的指令
SMIB,打开传
给终端的可
读但写保护
的文件
SMIB
S5
SMIB
控制处理
产生
随机数
向主机
发送值
S86
卡解密保密
密钥中的
随机数
解密
随机数
S66
解密
随机数
S76
将解密随
机数作为
密钥存储
安全模式
开启键盘

图 6F

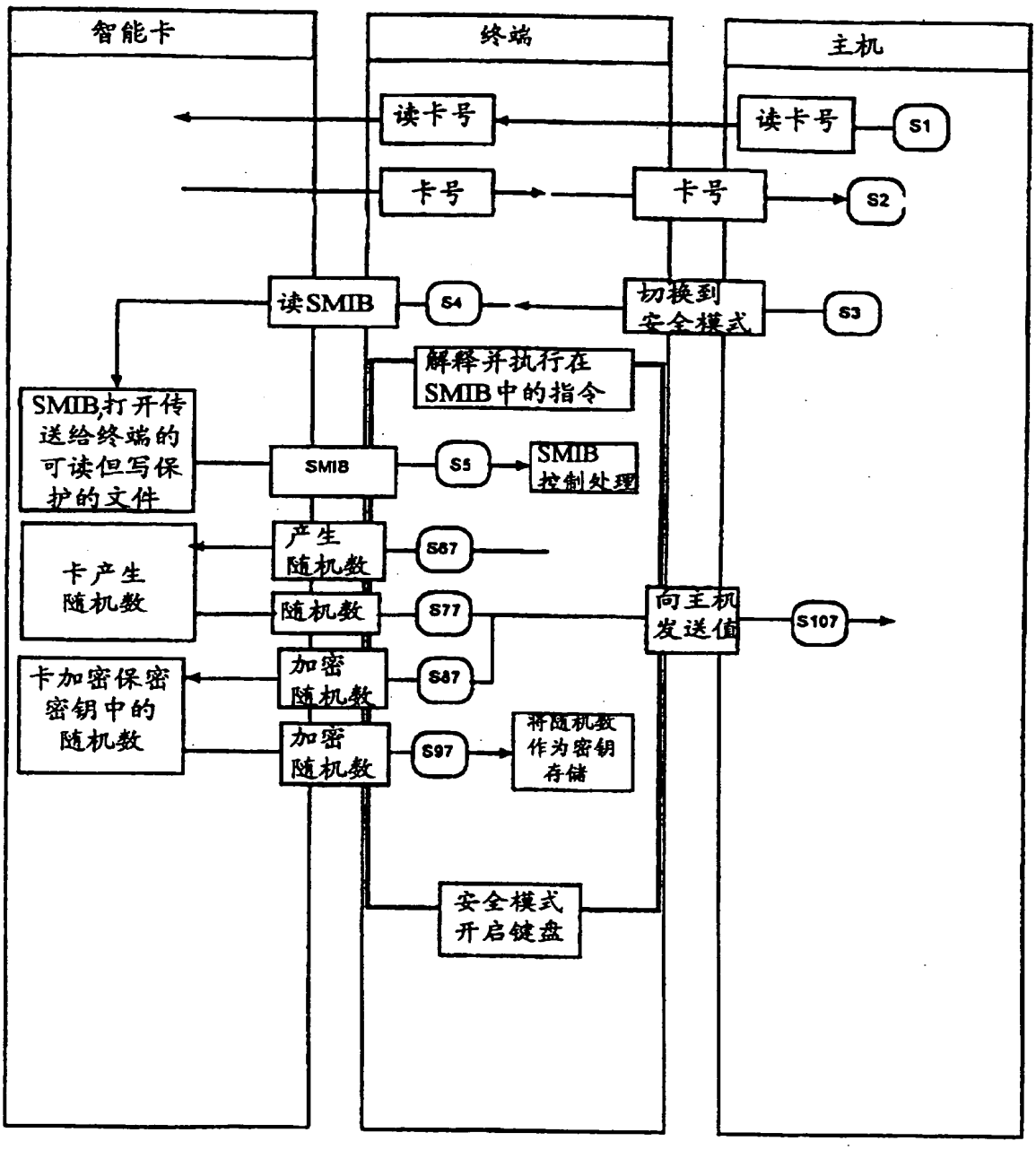

智能卡
终端
主机
读卡号
读卡号
S1
卡号
卡号
S2
读SMIB
S4
切换到
安全模式
S3
解释并执行在
SMIB中的指令
SMIB,打开传
送给终端的
可读但写保
护的文件
SMIB
S5
SMIB
控制处理
卡产生
随机数
产生
随机数
S67
随机数
S77
向主机
发送值
S107
卡加密保密
密钥中的
随机数
加密
随机数
S87
加密
随机数
S97
将随机数
作为密钥
存储
安全模式
开启键盘

图 6G

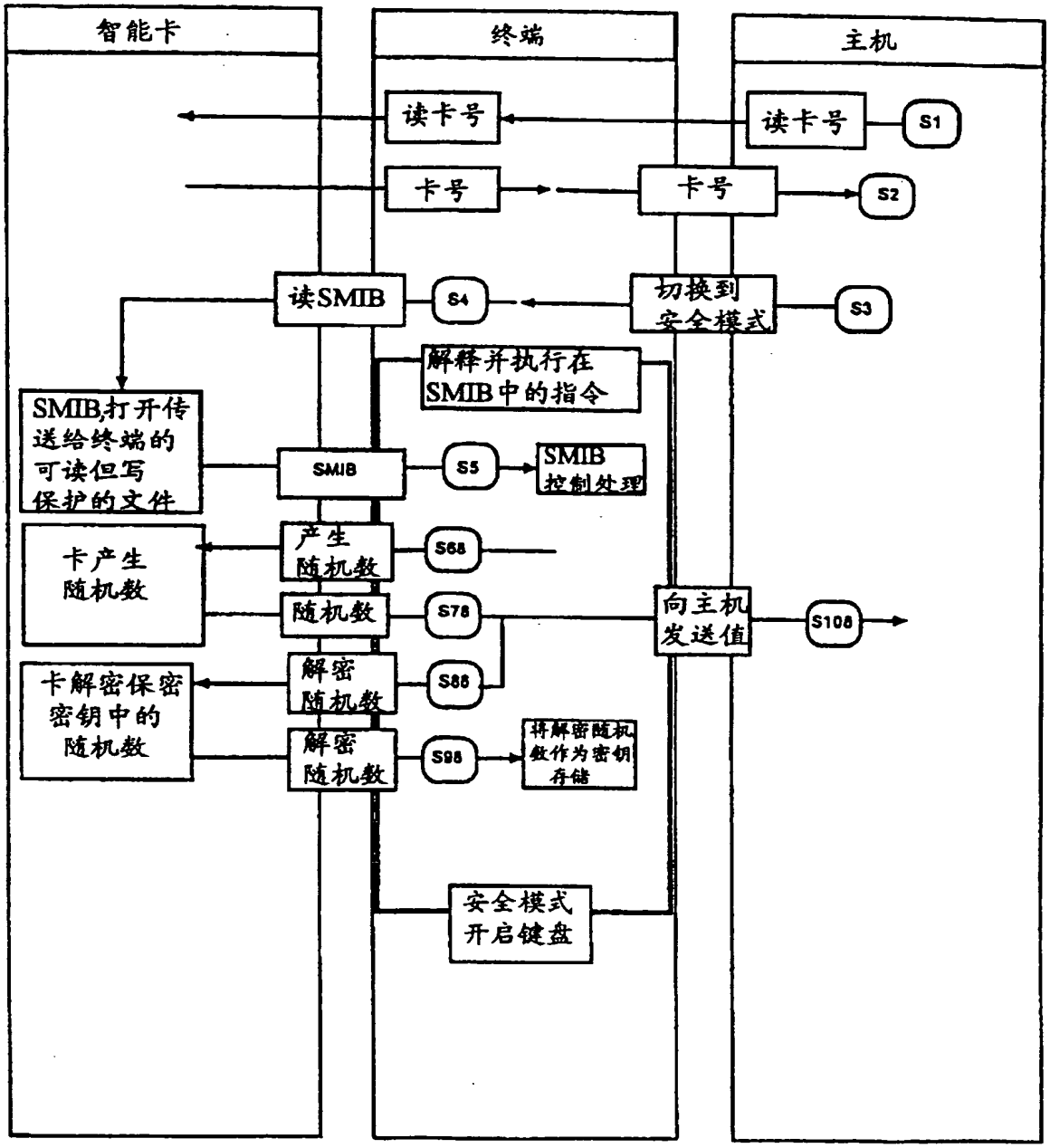

智能卡
终端
主机
读卡号
读卡号
S1
卡号
卡号
S2
读SMIB
S4
切换到
安全模式
S3
解释并执行在
SMIB中的指令
SMIB,打开传
送给终端的
可读但写
保护的文件
SMIB
S5
SMIB
控制处理
卡产生
随机数
产生
随机数
S68
随机数
S78
向主机
发送值
S108
卡解密保密
密钥中的
随机数
解密
随机数
S88
解密
随机数
S98
将解密随机
数作为密钥
存储
安全模式
开启键盘

图 6H